Software Requirements Specification (SRS) for Administration Services

Defense Information Infrastructure (DII)
Common Operating Environment (COE)

11 July 1997

V3.2

Section 1

SCOPE

1.1 Identification

This Software Requirement Specification (SRS) describes the Administration Services for the Defense Information Infrastructure (DII). Dependencies and interactions between the Administration Services and other functional areas of DII are discussed to help clarify where the Administration Services begin and end and how these services fit into the overall DII Common Operating Environment (COE) .

1.2 Administration Services Overview

Administration Services is defined as the ability to manage all hardware and software resources in a heterogeneous, distributed information system. Efficient and effective management of DII is extremely important to the functional user community supporting the defense of the United States. Maintaining operations of a vast and diverse array of information resources interconnected with Local Area Networks (LAN) and Wide Area Networks (WAN) is a major undertaking; however with strict guidelines and robust tools the task will be better handled. The purpose is to ensure that the information systems continue to operate in support of the efforts of the warfighters and supporting organizations during peace-time, crisis and war-time operations. This document addresses and defines the functions and requirements of the Administration Services within the DII COE.

Administration Services includes the following areas, which are often implemented separately due to the lack of integrated tools:

1) System Administration: System Administration is defined as the services that are required to ensure effective and efficient operation of those elements of the information system that are not an integral part of the network and to manage the configuration and operations of workstations, servers, applications and the user environment on a day-to-day basis.

2) Security Administration: Security Administration is defined as the services required to manage, configure, operate and maintain information system security functions and to ensure that the system continues to meet security requirements as defined by the accrediting authority.

3) Desktop Administration: Desktop Administration is defined as those services that support the configuration of user's desktop, which provides access to system functions and applications.

This Software Requirements Specification (SRS) identifies the functional requirements for Administration Services to support these three areas. Because these areas are interdependent, the requirements are addressed in terms of Administration Services as an integrated set of functions. These functions include the five System Management Functional Areas (SMFAs) defined by the International Organization for Standardization (ISO): configuration management, fault management, performance management, security management, and accounting management. However, since accounting management entails functions necessary for charging fees to users for the use of system resources, and it is not the intention of the government to need those capabilities, accounting management will not be addressed further in this document.

Administration Services are provided in accordance with Management Domains as defined by the ISO. A management domain is a bounded set of information system resources that are under the management and control of a single set of management tools. Three levels of management have been defined for DII: (descriptions of global, campus and site to be added). There is a single manager for the global level, while the campus and local levels will be implemented numerous times depending on Command and site configurations. Each implementation constitutes a management domain.

1.3 Document Overview

This document is divided into the major sections described below.

Section 2: Lists documents either referenced herein, or applicable to system management requirements.

Section 3: Specifies the functional areas of Administration Services and the requirements of each of those areas.

Section 4: Specifies the quality assurance methods necessary to ensure that the functional requirements have been met.

Section 5: Identifies the traceability of the requirements for the implementation of the software modules associated with each functional area.

Section 2

APPLICABLE DOCUMENTS

This section provides references to applicable documents that describe requirements, specifications and functional capabilities for system management.

2.1 Government Documents

1. Defense Information Infrastructure (DII) Common Operating Environment (COE) Baseline, Version 1.0, Preliminary Draft, February 14, 1996, Defense Information Systems Agency (DISA).

2. Defense Information Infrastructure (DII) Common Operating Environment (COE) Integration and Runtime Specification (I&RTS) , Version 2, October 23, 1995, DISA.

3. Defense Information Infrastructure (DII) Common Operating Environment (COE) Alerts Software Requirements Specification, DISA.

4. Defense Information Infrastructure (DII) Common Operating Environment (COE) Security Software Requirements Specification,Version 2.0, 8 July 1996, DISA.

2.2 Non-Government Documents

1. Internet Engineering Task Force (IETF) Internet Request for Comment (RFC) 1514 (Host Resources Management Information Base (MIB))

2. IETF RFC 1213 Network Protocols (MIB II).

3. ISO References

Section 3

REQUIREMENTS

Administration Services requirements are addressed in the following paragraphs. The requirements are discussed in terms of the four SMFAs defined by the ISO.

The Administration Services for DII provide automated support for the day-to-day operation and configuration of the DII COE workstations, servers, services, resources, and applications software. Management responsibilities are separated into two duty positions: a system administrator and a security administrator. Depending on the size of the specific installation, these positions may be filled by one or more personnel.

All management functions within the DII environment will be implemented using a manager-agent paradigm. The manager is software that is used to monitor and control system resources from a central location. Specific Administration Services are provided for configuration, fault, performance, and security management. The requirements for these Administration Services are discussed in the following subsections. Each resource to be monitored and controlled will have a management agent installed in it. The agent collects information for the manager, effects the changes the manager requests, and reports event or error conditions. Resources that do not have a native agent can still be managed via a proxy agent that acts as a go-between for the manager, translating the manager's requests into terms the resources can understand. Managers and agents are grouped into management domains, where the resources in a domain are managed by a single manager. The agents in the resources within a domain interact with the manager for that domain.

System management provides the capability for managing the DII system components (software and hardware). This includes the ability to control the versions of the software, software dependencies, hardware and hardware dependencies, user accounts and profiles, training and maintenance requirements. It also provides the capability to produce and review system utilization, system violation (i.e., invalid logins, viruses, threats), and system performance. It allows the system administrator to maintain the system in a properly configured environment.

Security management provides the capability for managing the DII security features. This includes the ability to control access to all DII workstations, servers, applications and data protection, audit trail, and real time threat information.

Desktop management provides the capability for managing the configuration of the DII desktop. This includes the ability to configure the desktop with icons and/or menus which

allow the user to access DII COE applications, system functions and objects in accordance with their profile.

3.1 Required States and Modes

The DII operates in the following modes:

• Operational Mode. This is the normal mode of operation where the DII is on-line supporting the operational mission.

• Maintenance Mode. In this mode, portions of the hardware or software at the DII site will be off-line for maintenance, modification, upgrade, or other related action.

• Training Mode. In this mode, a portion of the DII may be operated with separate databases using simulated inputs in support of training for a portion of the user population. Care must be taken to ensure that exercise data is not mixed with operational data.

• Exercise Mode. In this mode, a portion of the DII may be operated with separate databases using simulated inputs in support of an exercise for a portion of the user population.

Care must be taken to ensure that exercise data is not mixed with operational data. Normal day-to-day operations will probably find all four operating modes existing at the same time at different DII sites. The modes will be distinguished by administrative features or architectural boundaries. The Administration Services requirements are valid for all required states and modes.

3.2 Administration Services Requirements

Administration Services will incorporate the following functions for managing the network, system, and security of DII: Configuration Management, Fault Management, Performance Management, and Security Management. The requirements for these functions are specified in the following subsections:

3.2.1 Configuration Management
3.2.2 Fault Management
3.2.3 Performance Management
3.2.4 Security Management

The DII COE will employ an integrated management perspective for the individual DII sites. Management will be performed within a defined set of management domains, in

accordance with the DII System and Network Management Concept of Operations. Network management of the Defense Integrated Services Network (DISN) Secret Internet Protocol (IP) Router Network (SIPRNET) WAN will be performed separately by the Defense Information Systems Agency (DISA).

3.2.1 Configuration Management

Configuration Management includes functions to control the configuration of network, system or application entities. Configuration Management will provide automated tools for identifying, controlling and collecting data on DII resources for the purposes of determining status, user account management and auditing. These automated tools shall be available from any host as needed and as appropriate within the administrative domain. Additionally, these automated tools shall support multiple, simultaneous access by authorized administrators. Supporting this area are the functions to:

1. Create, delete, examine and change sets of management information that describe parts of a system.

2. Examine and be notified of changes in the state of the system to monitor overall operability and use of the system and give or withhold permission for the use of specific resources.

3. Examine the relationships among various parts of the system to see how the operation of one part of the system depends upon or is depended upon by other parts.

Configuration Management incorporates the following requirements for network, system and security components as it applies.

3.2.1.1 Administration Services shall comply with account group requirements as specified in the DII I&RTS. Account Groups are a set of logically related system functions provided by one or more COE segments. COE segments may provide system functions for one or more account groups.

3.2.1.2 Administration Services will support a master profile which defines the user configuration for all of the system functions contained within a base account group.

3.2.1.2.a The master profile shall be used as a template to create other profiles within an account group.

3.2.1.2.b The master profile shall not be assignable to a user, only those profiles that are created from the master profile template are assignable to users. Profiles may contain all or a subset of the system functions within a base account group.

3.2.1.2.c Profiles shall only contain system functions from one account group.

3.2.1.2.d The user's active profile(s) shall control the user's access to system functions (e.g., applications) within the user's session.

3.2.1.2.e The user's active profile(s) shall control the user's access to subfunctions within a system function (e.g., ability to access a certain function or object within an application) within the user's session.

3.2.1.2.f The user's active profile(s) shall control the user's access to system objects (e.g., files) within the user's session.

3.2.1.3 Administration Services shall provide a GUI-based capability for centralized profile creation with the capability to define the following parameters:

- Unique Profile Name (within administrative domain)
- Account Group
- System Function(s)
- Subfunctions of System Fucntion(s)
- Object Permissions

3.2.1.3.a The profile creation mechanism shall require the definition of the profile name and account group, as a minimum, in order to create the new profile.

3.2.1.3.b The definition of the system function(s), subfunctions of system function(s) and object permissions shall be optional.

3.2.1.4 The profile creation mechanism shall provide the capability to create new profiles from existing profiles, e.g., a “save-as” capability.

3.2.1.5 The profile creation mechanism shall be extensible such that it will support the execution of additional tasks during profile creation as required by the COE and its segments. These tasks may include the creation of a profile-based mail group, mail box and routing mechanism.

3.2.1.6 The profile creation mechanism shall be extensible such that it will support the execution of additional tasks during the assignment of a system function to a profile as required by the COE and its segments. These tasks may include the assignment of database privileges to a profile.

3.2.1.7 The profile creation mechanism shall be extensible such that it will support the execution of additional tasks during the deassignment of a system function to a profile as required by the COE and its segments. These tasks may include the deassignment of database privileges to a profile.

3.2.1.8 Administration Services shall provide a GUI-based capability for centralized profile modification with the capability to modify the following profile parameters:

- System Function(s)
- Subfunctions of System Fucntion(s)
- Object Permissions

3.2.1.9 Administration Services shall provide a GUI-based capability for centralized profile deletion. The profile deletion mechanism shall reverse all actions associated with profile creation including deassigning the deleted profile from all users who have been previously assigned the deleted profile.

3.2.1.10 The profile deletion mechanism shall be extensible such that it will support the execution of additional tasks during profile deletion as required by the

COE and its segments. These tasks may include the deletion of a profile-based mail group, mail box and routing mechanism.

3.2.1.11 Administration Services shall provide a GUI-based capability for centralized assignment of profile(s) to users with the capability to define the following parameters:

- User Identifier
- Profile(s)

3.2.1.12 The profile assignment mechanism shall be extensible such that it will support the execution of additional tasks during user profile assignment as required by the COE and its segments. These tasks may include adding a user to a profile-based mail group.

3.2.1.13 Administration Services shall provide a GUI-based capability for centralized deassignment of profile(s) to users. The profile deassignment mechanism will provide the capability to reverse all actions associated with assignment of profile(s) to users.

3.2.1.14 The profile deassignment mechanism shall be extensible such that it will support the execution of additional tasks during user profile deassignment as required by the COE and its segments. These tasks may include deleting a user from a profile-based mail group.

3.2.1.15 Administration Services shall provide the capability to automatically distribute or make available via network information services profile information to a single host, a group of hosts or all hosts within the administrative domain.

3.2.1.16 Administration Services shall provide a GUI-based profile selection mechanism with the following capabilities:

3.2.1.16.a The profile selection mechanism shall be available after successful user login should the user possess multiple profiles and the ability to select multiple profiles. The presentation of the profile selection mechanism shall be configurable such that it may be disabled by the administrator.

3.2.1.16.b The profile selection mechanism shall be available in the user's work environment to allow dynamic changing of profiles such that users may select additional profiles and deselect previously selected profiles.

3.2.1.16.c The profile selection mechanism shall display the user's valid profiles, currently selected profile(s) and unselected profile(s).

3.2.1.16.d The profile selection mechanism shall allow a configurable number of selections, either 1 or n, where the user may be restricted to selecting one profile only or can select any number of profiles up to n where n is the total number of valid profiles for the user.

3.2.1.16.e The profile selection mechanism shall allow an administrator to restrict the occupancy of a profile to one user in an administrative domain, e.g., the capability to lock a profile on a profile by profile basis.

3.2.1.17 The profile selection mechanism shall be extensible such that it will support the execution of additional tasks during user profile selection as required by the COE and its segments. These tasks may include providing the user with database access privileges based on the assumption of a profile.

3.2.1.18 The profile selection mechanism shall be extensible such that it will support the execution of additional tasks during user profile deselection as required by the COE and its segments. These tasks may include removing the user's database access privileges based on the deselection of a profile.

3.2.1.19 Administration Services shall provide a GUI-based capability for centralized user account creation in a heterogeneous environment with the capability to define the following user parameters:

- Unique user identifier (within administrative domain)
- Login name
- Initial password
- Home directory file server
- Group memberships
- Mail alias(es)
- Shell
- Other user information, e.g., user's real name, telephone

3.2.1.20 The user account creation mechanism shall be extensible such that it will support the execution of additional tasks during user account creation as required by the COE and its segments. These tasks may include adding users to the DBMS, Profile Database, and DCE Registry and creating user's home directory.

3.2.1.21 Administration Services shall create users such that it will support unitary login of the user.

3.2.1.22 Administration Services shall provide a unitary login capability to support transparent, distributed login for all users.

3.2.1.23 Administration Services shall provide a GUI-based capability for centralized user account modification in a heterogeneous environment with the capability to modify the following user parameters:

- Login name
- Password
- Home directory file server
- Group memberships
- Mail alias(es)
- Shell
- Other user information, e.g., user's real name, telephone

If the user's home directory file server is modified, the account modification mechanism shall create a new home directory on that server.

3.2.1.24 Administration Services shall provide a GUI-based capability for centralized user account deletion in a heterogeneous environment. The user account deletion mechanism will provide the capability to reverse all actions associated with user account creation. The account deletion mechanism shall prompt for user home directory deletion, with a default of "no".

3.2.1.25 The user account deletion mechanism shall be extensible such that it will support the execution of additional tasks during user account deletion as required by the COE and its segments. These tasks may include deleting users from the DBMS, Profile Database, and DCE Registry and deleting user's home directory.

3.2.1.26 Administration Services shall provide the capability to automatically distribute or make available via network information services user account information to a single host, a group of hosts or all hosts within the administrative domain.

3.2.1.27 Administration Services shall provide a GUI-based capability for centralized group creation in a heterogeneous environment with the capability to modify the following group parameters:

- Unique group identifier (within administrative domain)
- Group name
- Members

The group creation mechanism shall not be capable of creating account groups as defined in the DII I&RTS.

3.2.1.28 Administration Services shall provide a GUI-based capability for centralized group modification in a heterogeneous environment with the capability to modify the following group parameters:

- Group name
- Members

The group modification mechanism shall not be capable of modifying account groups as defined in the DII I&RTS.

3.2.1.29 Administration Services shall provide a GUI-based capability for centralized group deletion in a heterogeneous environment. The group account deletion mechanism will provide the capability to reverse all actions associated with group account creation.

The group deletion mechanism shall not be capable of deleting account groups as defined in the DII I&RTS.

3.2.1.30 Administration Services shall provide the capability to automatically distribute or make available via network information services group information to a single host, a group of hosts or all hosts within the administrative domain.

3.2.1.31 Administration Services shall provide a GUI-based capability for centralized host definition in a heterogeneous environment with the capability to define the following host parameters:

- Hostname
- IP Address
- Hostname aliases

3.2.1.32 Administration Services shall provide the capability to automatically distribute or make available via network information services host information to a single host, a group of hosts or all hosts within the administrative domain.

3.2.1.33 Administration Services shall provide a GUI-based capability to install software resources and patches from a central location on a single host, a group of hosts or all hosts within the administrative domain.

3.2.1.34 The software installation mechanism shall be extensible such that it will support the execution of additional tasks during software installation as required by the COE and its segments. These tasks may include identification of the system functions of the software, associating those system functions with account groups and updating the profile database with new system functions.

3.2.1.35 Administration Services shall provide a GUI-based capability to upgrade software resources and patches from a central location on a single host, a group of hosts or all hosts within the administrative domain.

3.2.1.36 The software upgrade mechanism shall be extensible such that it will support the execution of additional tasks during software upgrade as required by the COE and its segments. These tasks may include identification of the system functions of the software, associating those system functions with account groups and updating the profile database with new system functions.

3.2.1.37 Administration Services shall provide a GUI-based capability to deinstall software resources and patches from a central location on a single host, a group of hosts or all hosts within the administrative domain.

3.2.1.38 The software deinstallation mechanism shall be extensible such that it will support the execution of additional tasks during software de-installation as required by the COE and its segments. These tasks may include removal of

the system functions of the software from an account groups and updating the profile database.

3.2.1.39 Administration Services shall provide a GUI-based capability for centralized distribution of files and file packages (including directories of files) from a central location to a single host, a group of hosts or all hosts within the administrative domain.

3.2.1.40 Administration Services shall provide a GUI-based capability to centrally monitor and control print queues in a heterogeneous environment and perform the following administration tasks:

3.2.1.40.a Administration Services shall provide the capability to display the print queue.

3.2.1.40.b Administration Services shall provide the capability to start the print queue.

3.2.1.40.c Administration Services shall provide the capability to stop the print queue.

3.2.1.40.d Administration Services shall provide the capability to delete print jobs from the print queue.

3.2.1.40.e Administration Services shall provide the capability to prioritize print jobs in the print queue

3.2.1.40.f Administration Services shall provide the capability to move print jobs in the print queue.

3.2.1.40.g Administration Services shall provide the capability to move print jobs between print queues.

3.2.1.41 Administration Services shall provide a GUI-based capability to centrally monitor and control printer in a heterogeneous environment and perform the following administration tasks:

3.2.1.41.a Administration Services shall provide the capability to start printers.

3.2.1.41.b Administration Services shall provide the capability to stop printers.

3.2.1.41.c Administration Services shall provide the capability to flush printers.

3.2.1.42 Administration Services shall provide the capability to centrally create print queues in a heterogeneous environment within the administrative domain.

3.2.1.43 Administration Services shall provide the capability to centrally delete print queues in a heterogeneous environment within the administrative domain.

3.2.1.44 Administration Services shall provide the capability to create printer definitions for the printing system within the administrative domain with the capability to define the following parameters:

- Printer Name(s)
- Printer Type
- Print Server
- Printer Parameters (e.g., default, flow control)

3.2.1.45 Administration Services shall provide the capability to modify printer definitions in the printing system within the administrative domain with the capability to define the following parameters:

- Printer Name(s)
- Printer Type
- Print Server
- Printer Parameters (e.g., default, flow control)

3.2.1.46 Administration Services shall provide the capability to delete printer definitions from the printing system within the administrative domain. The printer deletion mechanism will provide the capability to reverse all actions associated with printer definition.

3.2.1.47 Administration Services shall provide the capability to automatically distribute or make available via network information services printer information to a single host, a group of hosts or all hosts within the administrative domain.

3.2.1.48 Administration Services shall provide a GUI-based capability for centralized monitor and control of processes in a heterogeneous environment and perform the following administration tasks:

3.2.1.48.a Administration Services shall provide the capability to display the status of processing resources.

3.2.1.48.b Administration Services shall provide the capability to identify active and failed processes.

3.2.1.48.c Administration Services shall provide the capability to terminate processes.

3.2.1.48.d Administration Services shall provide the capability to suspend processes.

3.2.1.48.e Administration Services shall provide the capability to resume processes.

3.2.1.48.f Administration Services shall provide the capability to send administrator-defined signals to processes, e.g., SIGHUP.

3.2.1.49 Administration Services shall provide the capability to control disk resources and perform the following administration tasks:

3.2.1.49.a Administration Services shall provide the capability to allocate user disk space including setting quotas.

3.2.1.49.b Administration Services shall provide the capability to modify disk partitions.

3.2.1.49.c Administration Services shall provide the capability to mount file systems.

3.2.1.49.d Administration Services shall provide the capability to unmount file systems.

3.2.1.49.e Administration Services shall provide the capability to determine disk space usage.

3.2.1.49.f Administration Services shall provide the capability to determine disk space availability.

3.2.1.49.g Administration Services shall provide the capability to create file systems.

3.2.1.49.h Administration Services shall provide the capability to modify file systems.

3.2.1.49.i Administration Services shall provide the capability to create file system tables.

3.2.1.49.j Administration Services shall provide the capability to modify file system tables.

3.2.1.49.k Administration Services shall provide the capability to export file system tables.

3.2.1.50 Administration Services shall provide the capability to specify a drift threshold for time synchronization across the administrative domain.

3.2.1.51 Administration Services shall provide the capability specify a synchronization method (e.g., abrupt, increase rate) for time synchronization across the administrative domain.

3.2.1.52 Administration Services shall provide the capability to monitor and control peripherals within the administrative domain (e.g., cdroms, printers, tape drives) and perform the following administration tasks:

3.2.1.52.a Administration Services shall provide the capability to allocate access to peripherals.

3.2.1.53 Administration Services shall provide the capability for centralized reboot and change of run state of a single host, a group of hosts or all hosts within the administrative domain.

3.2.1.54 Administration Services shall provide a GUI-based capability to centrally monitor and control system and application log files within the administrative domain and perform the following administration tasks:

3.2.1.54.a Administration Services shall provide the capability to view log files.

3.2.1.54.b Administration Services shall provide the capability to purge log files.

3.2.1.54.c Administration Services shall provide the capability to archive log files to a selected storage medium.

3.2.1.54.d Administration Services shall provide the capability to print logs files to a selected printer.

3.2.1.54.e Administration Services shall provide the capability to compress log files.

3.2.1.54.f Administration Services shall provide the capability to control the size of the log files.

3.2.1.54.g Administration Services shall provide the capability to enable/disable logging.

3.2.1.54.h Administration Services shall provide the capability to search log files.

3.2.1.55 Administration Services shall provide the capability to detect and identify all network addressable managed hardware resources within each management domain. This shall include, at a minimum, the following attributes:

- IP Address
- Name
- Location to nearest router
- Other information as available

3.2.1.56 Administration Services shall provide the capability to identify all managed software resources (e.g., segments) within each management domain. This shall include, at a minimum, the following attributes:

- Name
- Installation Location (e.g., installed host)
- Type
- Version and Release Number
- Patch Number
- Other information as available

3.2.1.57 Administration Services shall provide the capability to create a diagrammatic representation of the interconnected network resources within each management domain.

3.2.1.58 Administration Services shall provide the capability to update the diagrammatic representation of the interconnected network resources within each management domain.

3.2.1.59 Administration Services shall provide the capability to display and print a diagrammatic representation of the interconnected network resources within each management domain.

3.2.1.60 Administration Services shall provide the capability to detect and modify the configuration of hardware and software resources from a central location within the management domain. The manager shall be capable of detecting and modifying the attributes of managed objects implemented and used by host and network resources in the management domain. Each manager agent residing on a workstation, server or network device shall be capable of responding to requests from the manager to return the value of the attribute stated in the manager's request and to modify the current value of the attribute stated in the request. Managed objects shall be defined and their attributes managed in accordance with Internet Request for Comment (RFC) 1514 (Host Resources Management Information Base (MIB)) and RFC 1213 (MIB II).

RFC 1514 defines managed objects for workstations and servers. Workstations and servers in the DII COE shall implement the following groups of managed objects.

Mandatory Managed Groups:

- Host Resources System Group
- Host Resources Storage Group
- Host Resources Device Group

Optional Managed Groups:

- Host Resources Running Software Group
- Host Resources Running Software Performance
- Host Resources Installed Software Group

RFC 1213 defines the MIB II for network management protocols in TCP/IP-based networks. The MIB is defined in terms of groups of managed objects. If the semantics of a group is applicable to an implementation (i.e., a network device), then the devices shall implement all objects in that group. (This is guidance for managed agents, the managing server must implement all groups.)

For network devices, the managed groups are: System, Interfaces, Address Translation, IP, ICMP, TCP, UDP, EGP, Transmission and SNMP.

3.2.1.61 Administration Services shall provide the capability to view the network names and addresses of all managed objects in the management domain.

3.2.1.62 Administration Services shall provide the capability to assign network names and addresses of all managed objects in the management domain.

3.2.1.63 Administration Services shall provide the capability to modify network names and addresses of all managed objects in the management domain.

3.2.1.64 Administration Services shall provide the following automated capabilities to support the maintenance of the managed hardware inventory.

3.2.1.64.a Administration Services shall provide the capability to create information in a database of the managed hardware inventory to include, at a minimum, the following parameters:

- Manufacturer
- Type
- Model

3.2.1.64.b Administration Services shall provide the capability to modify information in a database of the managed hardware inventory to include, at a minimum, the following parameters:

- Manufacturer
- Type
- Model

3.2.1.64.c Administration Services shall provide the capability to delete information in a database of the managed hardware inventory to include, at a minimum, the following parameters:

- Manufacturer
- Type
- Model

3.2.1.64.d Administration Services shall provide the capability to report the status of the managed hardware inventory within the management domain on request. Separate reports shall be available for each type of equipment.

3.2.1.64.e Administration Services shall provide the capability to send an alert in accordance with the DII Alerts SRS automatically when managed hardware inventory levels fall below a manually set threshold. The default threshold value shall be one spare unit.

3.2.1.65 Administration Services shall provide the capability to monitor inventory status on software (to include versions, types and numbers) at any given time by use of automated inventory control software.

3.2.1.66 Administration Services shall provide the capability to report inventory status on software (to include versions, types and numbers) at any given time by use of automated inventory control software.

3.2.1.67 Administration Services shall provide the capability to configure the LAN ports selection on the workstation hardware.

3.2.1.68 Administration Services shall provide the capability to configure the workstation name and IP address.

3.2.2 Fault Management

Fault management encompasses the need for a proactive capability to monitor, detect, identify, analyze, isolate and correct problems related to abnormal behavior of managed resources within DII. An important design consideration of DII is that it will not contain any "single points of failure."

3.2.2.1 Agents shall report changes of status of managed objects to the manager of the associated management domain.

3.2.2.2 Administration Services shall provide the capability to detect the loss of managed objects within each management domain.

3.2.2.3 Administration Services shall provide the capability to locate a failed managed object within a LAN segment (i.e., to the nearest router).

3.2.2.4 Administration Services shall provide the capability to disable failed or malfunctioning managed objects.

3.2.2.5 Administration Services shall provide the capability to disable routers and bridges in order to isolate LAN segments.

3.2.2.6 Administration Services shall provide the capability to create an operational duplicate image on a hard disk from any other compatible hard disk on the network.

3.2.2.7 Administration Services shall provide the capability for centralized backup of the system files, selected files or raw partitions on the system to an off-line selectable device in an automated mode.

3.2.2.8 Administration Services shall provide the capability for centralized backup of the system files, selected files or raw partitions on the system to an off-line selectable device in a manual mode.

3.2.2.9 Administration Services shall provide the capability for centralized restore of the system files, selected files or raw partitions on the system from an off-line selectable device.

3.2.2.10 Administration Services shall provide the capability to perform backups on media which are in active use (e.g., hot backups).

3.2.2.11 Administration Services shall provide the capability to perform incremental backups of files that have been added or modified since the last incremental backup.

3.2.2.12 Administration Services shall provide the capability to schedule backups to occur at frequencies which are configurable by file type.

3.2.2.13 Administration Services shall not allow backups to overwrite previous backups without the operator explicitly allowing the deletion or overwrite of the previous backup.

3.2.2.14 Administration Services shall provide the capability to initiate an alert when connectivity to the LAN or WAN is lost after a configurable period of time.

3.2.2.15 Administration Services shall provide the capability to initiate an alert when a configurable threshold of the data storage capacity has been reached, e.g., 85%.

3.2.2.16 Administration Services shall provide the capability to automatically save data in working memory when a configurable threshold of data storage capacity has been reached, e.g., 95%.

3.2.2.17 Administration Services shall provide the capability to automatically suspend operations when a configurable threshold of data storage capacity has been reached, e.g., 95%.

3.2.2.18 Administration Services shall provide the capability to perform workstation diagnostics with user definable parameters in a manual or automatic mode.

3.2.2.19 Administration Services shall provide the capability to generate a systems diagnostic report.

3.2.2.20 Administration Services shall provide the capability to remotely or locally verify the correct configuration and software load of a workstation.

3.2.3 Performance Management

Monitoring and controlling the quality of network communications and ensuring satisfactory performance of system resources is a primary thrust of the Administration Services. This process involves the monitoring and analyzing, tuning and controlling, and reporting on

network and information system components to include the system as one entity. The monitoring and analyzing functions include establishing the monitoring environment, the performance indicators, and the generation of appropriate reports. Tuning and controlling functions include activation of controls in order to fine tune the performance of the network and information systems. Recognizing and diagnosing the performance deficiencies are considered to be a fundamental requirement for the performance of the system. Reports being generated can include monitoring, tuning, tracking, and trend analysis.

Performance management includes those functions necessary to ensure optimum performance of the system. This, of necessity, entails the capability to monitor and adjust each manageable object in the management domain.

3.2.3.1 Administration Services shall provide the capability to retrieve usage-related attributes from managed objects . This shall include, as a minimum, the following attributes:

- Processor load in terms of percent of maximum capacity
- Disk use in terms of percent of maximum capacity
- Memory use in terms of percent of maximum capacity
- Network load in terms of average and instantaneous bytes per second

3.2.3.2 Administration Services shall provide the capability to modify managed object attributes. This shall include, as a minimum, the following attributes:

- Routing tables
- Buffer sizes
- Timers
- Swap Space

3.2.3.3 Administration Services shall provide the capability to move files and applications among the servers within the management domain.

3.2.3.4 Administration Services shall generate an alert in accordance with the Alerts SRS when the physical disk usage in the management domain reaches a definable threshold set by the operator. The threshold shall have a default value of 80%.

3.2.3.5 Administration Services shall provide the capability to generate a summary of performance and utilization of each managed object within the management domain.

3.2.3.6 Administration Services shall provide the capability for a single user to authenticate (via the GUI-based login mechanism) and be presented with a list of valid profiles (via the GUI-based profile selection mechanism) in the DII COE within ten (10) seconds.

3.2.3.7 Administration Services shall provide the capability for a single user to select one or more profiles (via the GUI-based profile selection mechanism) and be presented with the appropriate session icons (via the common desktop environment) in the DII COE within twenty (20) seconds.

3.2.3.8 Administration Services shall provide the capability for a single user to change their profile(s) (via the GUI-based profile change mechanism) and be presented with the appropriate session icons (via the common desktop environment) in the DII COE within twenty (20) seconds.

3.2.3.9 Administration Services shall provide the capability for a single user to launch a profile-based application (via the common desktop environment) and be presented with the application in the DII COE within five (5) seconds.

3.2.3.10 Administration Services shall provide the capability for a single user to logout of their user session (via the GUI-based logout mechanism) in the DII COE within ten (10) seconds.

3.2.3.11 Administration Services shall provide the capability for an administrator to create a single user in the DII COE within four (4) minutes. Creating a user includes defining the following parameters in the appropriate files and databases in the DII COE:

- Unique user identifier
- Login name
- Initial password
- Home directory file server
- Group memberships
- Mail alias(es)
- Shell
- Other user information, e.g., user's real name, telephone
- Profiles
- Other parameters as required by the DII COE and its segments (e.g., DBMS registry, DCE registry)

3.2.3.12 Administration Services shall provide the capability for an administrator to create a single profile in the DII COE within two (2) minutes. Creating a profile includes defining the following parameters in the appropriate files and databases in the DII COE:

- Unique profile name
- Account Group
- System Function(s)
- Other parameters as required by the DII COE and its segments (e.g., DBMS permissions, DCE access controls)

3.2.4 Security Management

DII Security Management is derived from national security policy and DII mission requirements. The Administration Services safeguard against various real threats such as unauthorized information access, expanding authorized access without appropriate authorization, information destruction, denying service, etc. The Administration Services will operate in concert with the security management procedures of those systems supporting the DII, which can be the source of external threats. Administration Services must cover all areas of security to include authentication, access control, encryption, and the ensuing audit trails. Authorized users will monitor and control the mechanisms which exist to protect network resources and user information, using the automated tools provided by Administration Services.

Security management systems include functionality for key management, access control and audit. The centralized control of these functions may be implemented either in a security management center on one hardware platform, or in distributed security management centers, each covering a specific management function. In either case, the scope of security management will be constrained to be consistent with the management domains.

The security requirements outlined within this document are a reflection of the DII security policy and are applicable in assisting the DII Security Administrator in completing his/her operational mission through system availability, confidentiality, accountability and integrity.

Information system security encompasses four security services:

Accountability: The property that enables activities on a system to be traced to individuals who may then be held responsible.

Availability: The property of system resources and information being accessible and usable upon demand by an authorized entity.

Confidentiality: The property that information is not made available or disclosed to unauthorized individuals, entities, or processes.

Integrity: The property that information has not been altered or destroyed in an unauthorized manner.

3.2.4.1 Accountability

3.2.4.1.1 Administration Services shall provide the a GUI-based capability to check whether or not the DII COE components are operating in a secure mode in accordance with the DII Security Requirements and to perform the following administrative tasks:

3.2.4.1.1.a Administration Services shall provide the capability to ensure security relevant system files and directories do not have dangerous access permissions (e.g., world writable or world readable).

3.2.4.1.1.b Administration Services shall provide the capability to examine the boot commands to ensure that files or paths referenced are not world writable.

3.2.4.1.1.c Administration Services shall provide the capability to ensure system devices are not world writable or world readable and that file systems have not been shared without any restrictions.

3.2.4.1.1.d Administration Services shall provide the capability to analyze the local or network user database and flag accounts with improperly constructed passwords in accordance the DII Security SRS, improper number of fields, non-unique user identifiers, and blank lines.

3.2.4.1.1.e Administration Services shall provide the capability to analyze the local or network group database and flag accounts with improperly constructed passwords in accordance the DII Security SRS, improper number of fields, non-unique group identifiers, blank lines and groups with duplicative members.

3.2.4.1.1.f Administration Services shall provide the capability to analyze trusted access to the system.

3.2.4.1.1.g Administration Services shall provide the capability to examine user home directories and specific files in each home directory to ensure they are not world writable.

3.2.4.1.1.h Administration Services shall provide the capability to analyze the protection configuration provided by the system using a rule based expert system.

3.2.4.1.1.i Administration Services shall provide the capability to check passwords against various dictionaries and certain algorithmic permutations to identify passwords that are easy to guess using a trial and error methodology. The dictionaries and permutations to use shall be configurable.

3.2.4.1.1.j Administration Services shall provide the capability to determine the version level of important system binaries and identify those that have not had the most recent security patches applied.

3.2.4.1.1.k Administration Services shall provide the capability to check for unexpected file system corruption or security breaches using Cyclic Redundancy Checks (CRCs) and changes to a file's inode attributes.

3.2.4.1.1.l Administration Services shall provide the capability to measure intrusion detection by reporting changes to a file's RSA MD5 encryption signature.

3.2.4.1.2 Administration Services shall provide the capability to identify each authorized DII user with a unique identifier (e.g., username) within the management domain.

3.2.4.1.3 Administration Services shall provide the capability to enable/disable security-relevant audit events within the administrative domain.

3.2.4.1.4 Administration Services shall provide a GUI-based capability for centralized audit reduction in a heterogeneous environment with the capability to selectively filter the audit records in accordance with the DII Security Requirements.

3.2.4.1.5 Administration Services shall provide a GUI-based capability for centralized audit trail management with the capability to perform the following administrative tasks:

3.2.4.1.5.a Administration Services shall provide the capability to view the raw audit trail.

3.2.4.1.5.b Administration Services shall provide the capability to view the reduced audit trail.

3.2.4.1.5.c Administration Services shall provide the capability to backup the audit trail to a selectable device.

3.2.4.1.5.d Administration Services shall provide the capability to restore the audit trail from a selectable device

3.2.4.1.5.e Administration Services shall provide the capability to archive the audit trail to a selectable device.

3.2.4.1.5.f Administration Services shall provide the capability to delete the audit trail. The audit deletion capability will not delete the audit trail without verifying the action with the administrator.

3.2.4.1.6 Administration Services shall provide a GUI-based capability to assign passwords to users.

3.2.4.2 Availability

3.2.4.2.1 Administration Services shall support trusted roles as defined in the DII Security Requirements.

3.2.4.2.2 Administration Services shall limit the system functions assigned to a trusted role to those required to perform the trusted role effectively as defined in the DII I&RTS.

3.2.4.2.3 Administration Services shall prohibit security relevant functions from being assigned to non-trusted roles. Security relevant functions include those functions which may affect the implementation of the security policy within the DII COE.

3.2.4.3 Confidentiality

3.2.4.3.1 Administration Services shall provide a GUI-based capability to set the access permissions (e.g., read, write, execute, control, delete) of system resources

(e.g., files, directories and applications), and to associate those privileges with specific users.

3.2.4.3.2 Administration Services shall provide a GUI-based capability to set the access permissions (e.g., read, write, execute, control, delete) of system resources (e.g., files, directories and applications), and to associate those privileges with specific groups.

3.2.4.3.3 Administration Services shall provide a GUI-based capability to set the ownership of system resources (e.g., files, directories and applications).

3.2.4.3.4 Administration Services shall provide the capability to manage sensitivity labels and handling caveats used in marking printed output with sensitivity labels and handling caveats.

3.2.4.3.5 Administration Services shall provide the capability to enable or disable marking printed output with sensitivity labels and handling caveats.

3.2.4.3.6 Administration Services shall provide a GUI-based capability for creating a set of authorized sensitivity labels and handling caveat values for use in marking printed output.

3.2.4.3.7 Administration Services shall provide a GUI-based capability for modifying the set of authorized sensitivity labels and handling caveat values that are used in marking printed output.

3.2.4.3.8 Administration Services shall provide a GUI-based capability for deleting of the set of authorized sensitivity label and handling caveat values that are used in marking printed output.

3.2.4.4 Integrity

3.2.4.4.1 Administration Services shall provide the capability to scan the hard drive and other storage media for known malicious software, e.g., worms, viruses, trojan horses.

3.2.4.4.2 Administration Services shall provide the capability to remove from the hard drive and other storage media known malicious software, e.g., worms, viruses, trojan horses.

3.3 Administration Services External Interface Requirements

3.3.1 Interface Identification and Diagrams

3.3.2 Project-Unique Identifier of Interface

3.3.2.1 Administration Services shall provide a set of standard Application Program Interfaces (APIs) to the Security Administration (SA) tools, in order that mission applications and other COE software can access SA functionality using a non-vendor specific interface.

3.3.2.2 Administration Services shall provide an interface to the Database Management System (DBMS) module of the COE for user accounts and profiles and audit information requests.

3.3.2.3 Administration Services shall provide an interface to the Alert Services Module of the COE for all SA related failures.

3.3.2.4 Administration Services shall provide an interface to the Desktop Manager in the Presentation Services module of the COE for user session management and desktop management.

3.3.2.5 Administration Services shall provide an interface to the System Administration software components of individual applications to be used within the COE.

3.3.2.6 Administration Services shall provide an interface to the Office Automation functional area for office automation software packages.

3.3.2.7 Administration Services shall provide an interface to the Message Processing functional area for message receiving, logging, storage, retrieval, parsing, generation, coordination, transmission and delivery.

3.3.2.8 Administration Services shall provide an interface to the On-line support functional area for on-line support services.

3.3.2.9 Administration Services shall provide an interface to the File Management services for file access to mission applications.

3.3.2.10 Administration Services shall provide an interface to the Network Administration area to configure, operate and maintain local and wide area networks.

3.3.3 Administration Services Internal Interface Requirements

The design of the security administration internal interface has not been determined at this time. These requirements will be developed during the software design process.

3.3.4 Administration Services Internal Data Requirements

TBD

3.3.5 Adaptation Requirements

TBD

3.3.6 Safety Requirements

TBD

3.3.7 Security and Privacy Requirements

Administration Services will provide for the management of the network, system and security mechanisms and be comprised of a set of management application entities and a management communications protocol stack.

3.3.7.1 Administration Services capabilities shall be accreditable, initially for the system high mode of operation in a distributed network environment and a stand-alone environment.

3.3.7.2 The security management functions shall be logically separated from other management functions, such that only authorized users can access them.

3.3.7.3 Administration Services security devices shall operate under a common security policy. The security devices may; however, be controlled from different management centers and hence belong to different management domains.

3.3.8 Environment Requirements

The Administration Services shall execute on all hardware and software platforms support by the DII COE.

3.3.9 Computer Resource Requirements

3.3.9.1 Computer Hardware Requirements

3.3.9.2 Computer Software Requirements

3.3.10 Software Quality Factors

The design of the Administration Services tools shall be in line with any software quality factors identified in the contract or derived from higher level specification.

3.3.11 Design and Implementation Constraints

Dependencies on other software: Relational Data Base Management System (RDBMS), Data Manager software described in tool kit COE functions.

Operating System version: HP/UX 9.07, HP/UX 10.0, Solaris 2.4 and Solaris 2.5, IBM AIX 4.1 and Digital UNIX (Version is TBD), Windows NT v3.51, Windows ‘95

Functions must operate in a distributed client/server computing environment.

3.3.12 Personnel-related Requirements

3.3.13 Training-related Requirements

3.3.14 Logistics-related Requirements

3.3.15 Other Requirements

None

3.3.16 Packaging Requirements

3.3.17 Precedence and Criticality of Requirements

The order of precedence or criticality indicating the relative importance of the requirements in this specification are identified and prioritized in Section 5, Requirements Traceability.

Section 4

QUALIFICATION PROVISIONS

This section identifies the qualification provisions including the methods used to ensure that the requirements in Section 3 have been met.

4.1 Qualification Methods

COE Software will be qualified through formal validation tests of the SRS level requirements. The Qualification Methods applied to the software shall include test, demonstration, analysis, and inspection (T, D, A, I).

4.1.1 Test

A qualification method that is carried out by operation of the item/component/interface (or some part of the computer software configuration item, etc.), and that relies on the collection and subsequent examination of data.

4.1.2 Demonstration

A qualification method that is carried out by operation of the Item/component/interface (or some part of the software configuration item, etc.), and that relies on observable functional operation not requiring the use of elaborate instrumentation or special test equipment.

4.1.3 Analysis

A qualification method that is carried out by the processing of accumulated data.

4.1.4 Inspection

A qualification method that is carried out by visual examination, physical manipulation, or measurement to verify that the requirements have been satisfied.

4.2 Special Qualification Requirements

TBD

Section 5

REQUIREMENTS TRACEABILITY

Section 6

NOTES

6.1 Acronyms and Abbreviations

COE	Common Operating Environment
DII	Defense Information Infrastructure
DISA	Defense Information Agency
DISN	Defense Integrated Services Network
ISO	International Organization for Standardization
LAN	Local Area Networks
MS	Administration Services
RPC	Remote Procedure Call
SIPRNET	Secret Internet Protocol Router Network
SMFA	System Management Functional Areas
SNMP	Simple Network Management Protocol
SRS	Software Requirements Specification
WAN	Wide Area Networks

6.2 Glossary

Account Group	Account Groups are a set of logically related system functions provided by one or more COE segments. COE segments may provide system functions for one or more account groups
Application	An application is an executable program that can be launched from a desktop icon.
Administrative Domain	The set of computing platforms and their associated resources (e.g., users, profiles, segments) that are under the administrative control of a single entity

Managed Object	ISO Reference
Management Domain	ISO Reference
Profile	A profile defines the user configuration or a subset thereof contained within an account group. User configuration encompasses the definition of icons, menu structure, group membership, and environmental variables needed to successfully execute the system function within an account group. A master profile exists for each account group and contains the user configuration for all of the system functions in the account group. Note: A user is assigned one or more profiles based on the systems functions the user will need to perform his/her functional activities.
Session	The implementation of the user's profile(s) within the user's work environment from login to logout. The session provides the resources that the user needs to perform the functions included in the user's profile(s).
System Function	A system function is an executable program or function within the program that may be represented by an icon on the desktop or a menu item in the menuing structure. A COE segment provides one or more system functions. An application or a separable function within an application is a system function.
Trusted Role	A trusted role is a profile in which the system functions assigned to that profile may affect the implementation of the security policy within the system.